Information Security Management System (ISMS)

Data Protection and Privacy Policy

DATA PROTECTION AND PRIVACY POLICY

1.1 Purpose

The purpose of this policy is to ensure data protection and privacy as required by contractual clauses with the organization's customers, vendors, and other third parties as well as to establish standards of compliance with global and domestic data privacy laws.

Furthermore, Esicia Limited takes its responsibilities with regard to the management of the requirements of Information security management (ISMS based on ISO 27001:2013) very seriously. This policy sets out how the organization manages those responsibilities.

Esicia Limited obtains, uses, stores, and otherwise processes personal data relating to current staff and customers, potential staff and customers, former staff and customers, contractors, and contacts, collectively referred to in this policy as data subjects. When processing personal data, the Organization is obliged to fulfill individuals' reasonable expectations of privacy by complying with ISO 27001 standards and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

1. Are clear about how personal data must be processed and the organization's expectations for all those who process personal data on its behalf;

2. Comply with the data protection law and with good practice;

3. Protect the organization's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights.

4. Protect the organization from risks of personal data breaches and other breaches of data protection law.

1.2 Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the organization's behalf must read it. A failure to comply with this policy may result in disciplinary action or termination of the contract.

All staff are responsible for ensuring that all organization staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls, and training to ensure that compliance.

The Information Security Unit is responsible for overseeing this policy.

1.3 Accountability

Esicia Limited must implement appropriate technical and organizational measures in an effective manner to ensure compliance with data protection principles. The organization is responsible for and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure compliance including:

1. appointing a suitably qualified representative;

2. Implementing privacy by design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;

3. integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing, and records of Personal Data Breaches;

4. Training staff on compliance with Data Protection Law and keeping a record accordingly; and

5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement efforts.

1.4 Responsibilities

1. Esicia Limited's responsibilities

As the Data Controller, the organization is responsible for establishing policies and procedures in order to comply with data protection law.

2. Network and Security department responsibilities

The Network & Security is responsible for:

(a) Advising the organization and its staff of its obligations under data protection and privacy policy.

(b) Monitoring compliance with this Regulation and other relevant data protection laws, the organization’s policies with respect to this

(c) To provide advice where requested on data protection impact assessments.

(e) the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context, and purposes of the processing.

3. Staff responsibilities

Staff members who process personal data about customers, staff, or any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) All personal data is kept securely;

(b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party;

(c) Personal data is kept in accordance with the organization's retention schedule;

(d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Security, and Conduct & Compliance teams;

(e) Any data protection breaches are swiftly brought to the attention of the Information Security, and Conduct & Compliance teams and the Network & Security that they support the Information Compliance team in resolving breaches;

(f) Where there is uncertainty around a data protection matter advice is sought from the Information Compliance teams and the Network & Security team.

4. Third-Party Data Processors

Where external companies are used to process personal data on behalf of the organization, responsibility for the security and appropriate use of that data remains with the organization.

Where a third-party data processor is used:

(a) A data processor must be chosen that provides sufficient guarantees about its security measures to protect the processing of personal data;

(b) Reasonable steps must be taken that such security measures are in place;

(c) A written contract establishing what personal data will be processed and for what purpose must be set out;

(d) A data processing agreement, available from the Information Compliance team, must be signed by both parties.

2.0 POLICIES

2.1 Policy Statements

2.1.1 The organization shall exercise legal ownership of the contents of all files stored on its computer and network systems as well as all messages transmitted via these systems.

2.1.2 The organization reserves the right to access information stored on any computer system connected to the corporate network without prior notice.

2.1.3 Data must be classified into different levels of sensitivity classifications with appropriate handling requirements in line with the information classification framework of the organization. This standard data sensitivity classification system must be used throughout the organization

2.1.4 The organization's entire internal information must be protected from disclosure to third parties.

2.1.5 Human Resources Management must ensure that all employees are fully aware of their legal and corporate responsibilities concerning the inappropriate sharing and releasing of information both internally within the organization and to external parties.

2.1.6 Prior to sending information to third parties, not only must the intended recipient be authorized to receive such information, but also the procedures and information security measures adopted by the third party must be seen to continue to assure the confidentiality and integrity of the information.

2.1.7 Data must be protected against unauthorized access or accidental changes and may only be deleted with the appropriate authorization.

2.1.8 Staff in custody of the organization's sensitive information must take appropriate steps to ensure that these materials are not available to unauthorized persons.

2.1.9 Confidential information must only be disclosed after express authorization has been obtained from the Data Owners or a legal/regulatory requirement in line with the organization's policies. Users permitted to access to such information are not permitted to disclose them to others.

2.1.10 If sensitive information is to be stored on the hard disk drive or other internal components of a personal computer, it must be protected appropriately.

2.1.11 Information classified as confidential must never be sent to a network printer without there being an authorized person to safeguard its confidentiality during and after printing.

2.1.12 when sensitive information is written to a magnetic disk or other storage media? the media must be suitably marked with the highest relevant sensitivity classification. If the marking constitutes an exposure, then such tapes must be kept in secured compartments without marking. When not in use, this media must be stored in locked safes.

2.1.13 An explicit statement describing exactly what information is restricted and how this information may be used must accompany all disclosures of confidential organization information to third parties.

2.1.14 Organization employees are prohibited from disclosing to anyone outside of the organization the nature of customer projects, customer business and marketing strategies, or customer business relationships.

2.1.15 Permission to disclose any internal Organization information to the news media or other third parties must be obtained from the Chief Executive Officer prior to release.

2.1.16 Staff must not sign confidentiality agreements provided by third parties without the advance authorization of the Legal office designated to handle intellectual property matters.

2.1.17 Activities requiring access to sensitive organization information must only be performed by full-time permanent employees unless one of the following conditions prevail:

- ✓ The requisite knowledge or skills are not possessed by a full-time permanent employee,
- ✓ An emergency or disaster requires the use of additional staff, or permission of Executive Management has been obtained.

2.1.18 Persons other than those specifically invited must not attend meetings where confidential information will be discussed.

2.1.19 If confidential information is released orally at a meeting or related presentation, the speaker must clearly communicate the sensitivity of the information and the need for discretion on the part of the audience. Visual aids such as slides and overhead transparencies must also include the appropriate confidentiality markings.

2.1.20 When sensitive information has been recorded on black boards or white boards, it must be definitively erased (with water or special cleaning fluids) before the authorized recipients of this information leave the area.

2.1.21 The data Centre's physical address is confidential and must not be disclosed to those without a demonstrable need-to-know.

2.1.22 Unauthorized access to the private user files and folders on organization's network and computer systems is prohibited.

2.1.23 Never lend to others a personal computer, handheld computer, transportable computer, smartphone, or any other computer that you use for business activities if the machine contains sensitive information.

2.1.24 Employees must lock all sensitive file cabinets and must provide a backup copy of the key(s) to their department manager.

2.1.25 The internal system addresses, configurations, and related system design information for the organization's networked computer systems must be restricted such that both systems and users outside the organization's internal network cannot access this information.

2.1.26 Personal data must not be retained longer than required

2.2 Personal Data Protection Principles

When you process personal data, you should be guided by the following principles, which are set out in the ISO 27001 Standard. The organization is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

1. processed lawfully, fairly, and in a transparent manner (Lawfulness, fairness, and transparency).

2. Collected only for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).

3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed (Data minimization).

4. Accurate and where necessary kept up to date (Accuracy).

5. Not kept in a form, which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).

6. Processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage (Security, integrity, and confidentiality).

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. Where the legal basis of our processing is Consent, to withdraw that consent at any time;

2. To ask for access to the personal data that we hold

3. To prevent our use of personal data for direct marketing purposes

4. To object to our processing of personal data in limited circumstances

5. To ask us to erase personal data immediately:

a) if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
b) if the only legal basis of the processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;

c) if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
d) if the data subject has objected to our processing for direct marketing purposes;
e) If the processing is unlawful.

6. To ask us to rectify inaccurate data or to complete incomplete data;

7. To restrict processing in specific circumstances e.g., where there is a complaint about accuracy;

8. the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the Organization; it is based on the data subject's explicit consent and is subject to safeguards; or is authorized by law and is also subject to safeguards;

9. To prevent processing that is likely to cause damage or distress to the data subject or anyone else;

10. To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

11. To make a complaint to the Network and Security; and

12. In limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. another organization) in a structured, commonly used, and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed

Requests (including for data subject access – see below) must be complied with, usually within one month of receipt.

You must immediately forward any Data Subject Access Request you receive to the Information Security and Conduct & Compliance Teams.

A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

Guidelines

- ❖ Third parties may be given access to the organization's internal information only when a demonstrable need-to-know exists, and when such a disclosure has been expressly authorized by the Data Owners and or a legal/regulatory requirement in line with the organization's policies.
- ❖ Protection for sensitive information may be by either a password access control package or encryption.

- As a general rule, information security policies and procedures should be revealed to only organization staff and select, outsiders (such as auditors) who have a legitimate business need for this information.
- Although certain marketing information is customarily disclosed to outsiders, they should never be disclosed to competitors. Likewise, marketing strategies, marketing plans, market share status, and other marketing information should never be shared with competitors.
- Systems administrators are authorized to examine private user files to handle emergencies such as virus infestations and system crashes. Whenever user files are to be examined in this manner, the involved user(s) should be notified. After the problem has been resolved, all copies of such files made by the administrator should be promptly destroyed.
- In order to maintain security and to prevent processing in infringement of Regulation, (as a data controller or processor) we would evaluate the risks inherent in processing collected personally identifiable data and implement measures to mitigate those risks, this could be by encryption and restricted access.
- A Data Protection responsible shall be designated.
- Highlights of the privacy policy may be published on the organization's corporate website.

- The organization's data classification is as follows:
  - ✓ CONFIDENTIAL

    This classification refers to highly sensitive internal documents, which could seriously damage the organization if lost or made public. Information classified as Confidential has very restricted distribution and must be protected at all times. Security at this level is the highest possible. Examples include impending mergers or acquisitions, corporate plans, or designs.
  - ✓ INTERNAL USE

    This classification refers to Information not approved for general circulation outside the organization where its disclosure would inconvenience the organization or management but is unlikely to result in financial loss or serious damage to credibility. Examples include internal memos, minutes of meetings, and internal project reports. Security at this level is controlled but normal.
  - ✓ PUBLIC

    This classification applies to all information meant for public use. Their disclosure will not adversely impact Esicia Limited, its employees, its stakeholders, its business partners, and/or its customers. Examples include newsletters, annual reports, published financial statements, etc. Security at this level is minimal.